REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
	Technical Report	-

4. TITLE AND SUBTITLE
Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

5a. CONTRACT NUMBER
W911NF-10-1-0416

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0D10BH

6. AUTHORS
Karl Berggren, Jeffrey Shapiro, Chee Wei Wong, Dirk Englund, Franco Wong, Gregory Wornell

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Columbia University
615 West 131 Street
Room 254, Mail Code 8725
New York, NY 10027 -7922

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58496-PH-DRP.14

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
We report on the theoretical and experimental progress, including the development of a large-alphabet quantum key distribution protocol that uses measurements in mu- tually unbiased bases. We also describe recent work for fine-key length analysis of the dispersive-optics QKD protocol, as well as security analysis based on the Franson interferometry measurement.

15. SUBJECT TERMS
quantum key distrubution, integrated photonic circuits

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dirk Englund
UU	UU	UU	UU		19b. TELEPHONE NUMBER 617-324-7014

Report Title

Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

ABSTRACT

We report on the theoretical and experimental progress, including the development of a large-alphabet quantum key distribution protocol that uses measurements in mu- tually unbiased bases. We also describe recent work for fine-key length analysis of the dispersive-optics QKD protocol, as well as security analysis based on the Franson interferometry measurement.

Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

Dirk Englund, Karl Berggren, Jeffrey Shapiro, Chee Wei Wong,
Franco Wong, and Gregory Wornell

Abstract

We report on the theoretical and experimental progress, including the development of a large-alphabet quantum key distribution protocol that uses measurements in mutually unbiased bases. We also describe recent work for fine-key length analysis of the dispersive-optics QKD protocol, as well as security analysis based on the Franson interferometry measurement.

Contents

1 Introduction

There has been rapid progress in developing optical quantum technologies that address unsolved problems in communications, computation, and metrology. Quantum key distribution now makes it possible to transmit information with absolute, unconditional security. These technologies require sophisticated electro-optic circuits, which are presently implemented in large custom-made bulk optics. There now exists an opportunity to translate optical quantum technologies from meter-sized table-top experiments to scalable sub-mm monolithic photonic integrated chips (PICs), leveraging recent advances in integrated optics. We combine quantum information processing (QIP) and PIC technology and a quantum photonic integrated chip (QPIC) architecture, offering densely integrated optical and electronic circuits into a rapidly reconfigurable platform. This technology will enable us to implement a novel high-dimensional dispersive optics quantum key distribution (DO-QKD) protocol [1]. The DO-QKD protocol enables the generation of a secret key between two parties Alice and Bob using high-dimensional photon encoding that enables information capacity in excess of 10 bits per photon. Working at the low-energy limit of secure communication, we will also investigate how telecom technology can be leveraged to approach the classical information capacity of optical channels under bandwidth and optical power constraints.

This update focuses on (Section 2) theoretical advances of the QKD protocol, including finite-key length analysis for the DO-QKD protocol and security analysis using the Franson interferometer, as well as experimental advances (Section 3).

2 Protocol Development

2.1 Achieving multiple secure bits per coincidence in time-energy entanglement based quantum key distribution

High-dimensional quantum key distribution (HDQKD) can potentially lead to high photon information efficiency and speed up the secure-key rate (SKR). Now, the groups of Jeffrey Shapiro and Franco Wong with postdoc Zheshen Zhang have proven that time-energy entanglement (TEE) based HDQKD is secure against collective attacks. The security rests upon the visibilities of the Franson and conjugate-Franson interferometers. We show that these visibilities allow for extracting the signal-idler arrival-time and frequency correlations, which are later exploited to upper bound eavesdropper's accessible information. In conjunction with the decoy-state approach, TEE based HDQKD promises over 200 km transmission distance in fiber and can achieve multiple secure bits per coincidence. This analysis is described in a manuscript to be submitted shortly [2].

2.2 Extended dispersive-optics QKD (DO-QKD) protocol

We have refined the security analysis of the DO-QKD protocol to not only protect against collective attacks [1], but are now also considering an extension to protect against coherent attacks. The extended analysis is expected to be completed by mid-February.

2.3 Analysis of non-local correlations of entangled photon pairs for arbitrary dispersion

Our analysis in the DO-QKD protocol was restricted so far to group velocity dispersion alone. However, optical materials typically also have higher order dispersion. In the past three months, we have arbitrary dispersion and focused in particular on dispersion in multi-spectral elements, such as optics found in wavelength division multiplexing systems. In contrast to the single, narrow coincidence peak yielded in Franson's nonlocal cancellation of single-channel dispersion, we have found that photon pairs, experiencing multi-frequency-channel,opposite dispersion, generally result in double coincidence peaks, which have the following properties: (1) each peak is as narrow as the coincidence peak with no dispersion; (2) while the biphoton spectrum sweeps over channels, the relative intensities of these two peaks change complementarily but the time difference between these two peaks remains constant. Understanding and using this effect are particularly important for high-dimensional QKD systems [3].

2.4 Finite-key security for dispersive optics QKD

The security proof for dispersive optics QKD [1] relies on the asymptotic limit—Alice's and Bob's keys were assumed to be infinitely long. To demonstrate security for finite-length keys, we are extending a security proof by Sheridan and Scarani [4, 5], treating DO-QKD as a discretized continuous-variable (CV) protocol and see in what limits the [4, 5] analysis is also valid for DO-QKD.

Ref. [4, 5] assumes a flat error rate; that is, for dimension d and total error rate Q, the probability that Alice and Bob measure the same character x is $p(x,x) = \frac{1-Q}{d}$, and the probability that Alice and Bob measure different characters x and y is $p(x,y) = \frac{1-Q}{d(d-1)}$.

The finite-size secret key rate is given by Eqn. (11) of [4] and reproduced here:

$$r_N = \frac{n}{N}\left(\min_{E|\mathbf{V}\pm\mathbf{\Delta V}} H(A|E) - H(A|B) - \frac{1}{n}\log\frac{2}{\varepsilon_{EC}} - \frac{2}{n}\log\frac{1}{\varepsilon_{PA}} - (2\log d + 3)\sqrt{\frac{\log(2/\bar{\varepsilon})}{n}}\right). \tag{1}$$

The first two terms, $\min_{E|\mathbf{V}\pm\mathbf{\Delta V}} H(A|E) - H(A|B)$, are pretty much analogous to the secure key capacity that we are currently calculating for DO-QKD. These first two terms include corrections due to fluctuations ΔV in the estimates of the error rates: $\Delta V = \Delta V(\varepsilon_{PE})$. The fluctuations are calculated from Eq. 12 of [4]. The third, fourth, and fifth terms of Eqn. (1) are corrections due to the possibility of failure of error correction, privacy amplification, and the use of smooth Renyi entropies (required for finite-key mathematical estimates), respectively. The factor n/N is due to the fact that for keys of total length N, a fraction of the key must be used for parameter estimation, leaving only n characters in the secret part of the key.

Ref. [4, 5] also assumes asymmetric basis selection; that is, Alice and Bob choose between the two measurement bases with unequal probabilities. One basis, U_{01} is selected with a much greater probability, p_{01}, than the other basis, U_{10}: $p_{01} > p_{10}$. When Alice and Bob both choose basis U_{01}, the resulting measurements are used to form the key, and when they both choose the other basis, the resulting measurements are used for parameter estimation.

It is also important to note that Ref. [4, 5] uses N to refer to the total number of signals exchanged by Alice and Bob, not the length of their keys. The length of Alice's and Bob's final keys is $n = Np_{01}^2$ words, and the number of words used for parameter estimation is $m = Np_{10}^2$. In a previous memo, we used N to denote the length of Alice's and Bob's keys. Hereafter, to enable comparisons with Ref. [4, 5], N will refer to the number of signals exchanged by Alice and Bob, and the length of Alice's and Bob's keys in DO-QKD will be denoted by $L = N/4$, where the factor $1/4$ comes from the fact that in DO-QKD, Alice and Bob choose between the two measurement bases with equal probabilities.

We compare the finite-size secure key capacity of DO-QKD to Ref. [4, 5] rates given by Eqn. (1). We subtract the correction terms from the asymptotic secure key capacity, $r_{\infty,DO}$ [1], and multiply the result by the secret fraction $L_{secret}/L = F(L)$, the fraction of the key that remains after part of it has been sacrificed for error rate estimation. (The calculation of $F(L)$ has been described in a previous memo.) Thus,

$$r_{N,DO} = F(L)\left(r_{\infty,DO} - \frac{1}{L_{secret}}\log\frac{2}{\varepsilon_{EC}} - \frac{2}{L_{secret}}\log\frac{1}{\varepsilon_{PA}} - (2\log d + 3)\sqrt{\frac{\log(2/\bar{\varepsilon})}{L_{secret}}}\right). \quad (2)$$

There are two versions of the DO-QKD secure key capacities. The first, ConstRate, keeps the alphabet time constant for all d. The implication for the calculation is that the probability of dark counts is the same for all d but the detector jitter $\propto 1/d$. The second version, FillSpace, keeps the bin time constant for all d, which means that the probability of dark counts $\propto d$ and the detector jitter is constant for all d.

The three parameters at our disposal are ϵ, η, and jitter. 'Jitter' refers to the base amount of jitter; in the ConstRate calculation, the base jitter is also multiplied by $1/d$. We are interested in knowing what ranges of these parameters match the rates in Ref. [4, 5]. When comparing, there are two particular quantities of interest: the asymptotic values of the rates and the value of N at which they become non-negative.

2.5 Comparing asymptotic values

For all values of ϵ and η and all $d > 2$, the asymptotic ConstRate value is greater than the asymptotic FillSpace value.

To make the asymptotic values somewhat agree, we require $\epsilon \sim 10^{-4}$ and $\eta \sim 10^{-4}$. Using $\epsilon = \eta = 10^{-4}$, the asymptotic DO-QKD values are about equal to the values for $d = 2$ discrete-variable QKD, but as d increases, the difference between the Ref. [4, 5] value and the DO-QKD values widens. See Fig. 1.

As the jitter increases, the asymptotic DO-QKD values decrease, but 1) the ConstRate values do not decrease as much as the FillSpace values do, and 2) the asymptotic ConstRate values are more resilient to increases in jitter as d increases.

For comparison, we can calculate the DO-QKD secure key capacity keeping both jitter and probability of dark counts constant for all d. In this case, the trend continues: the difference between the asymptotic Ref. [4, 5] values and the asymptotic DO-QKD values still increases as d increases (and the discrete variable QKD [4, 5] values are greater).

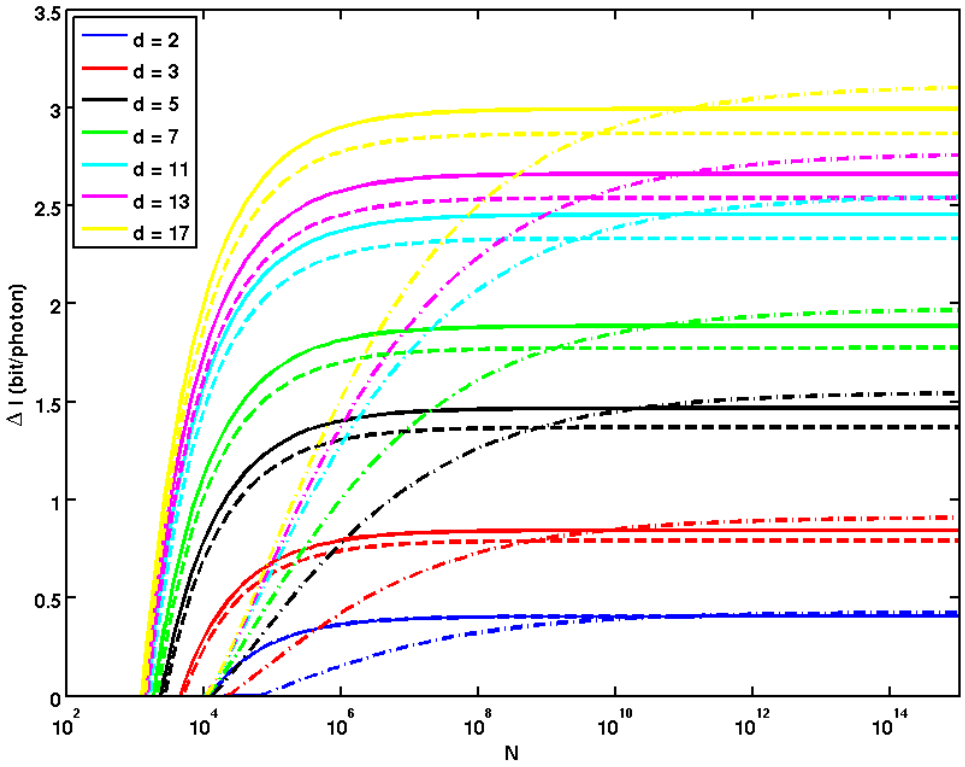

Figure 1: Plot of DO-QKD finite-size secure key capacities compared to finite-size secure key rates of Ref. [4, 5]. Lines of the same color all correspond to the same d. Solid lines represent DO-QKD ConstRate. Dashed lines represent DO-QKD FillSpace. Dash-dotted lines represent Ref. [4, 5], replicating Fig. 1 of [4]. The DO-QKD plots were constructed using $\eta = \epsilon = 10^{-4}$ and jitter $= 2\sigma_{cor}/3$, where σ_{cor} is the correlation time.

2.6 Comparing behavior for low N

Ref. [4, 5] and most other finite-key security proofs agree that in order to have a positive secure key capacity, $N > 10^5$ signals must be exchanged [4, 6]. For low N, we see that DO-QKD differs from discrete variable QKD in two ways: 1) the secure key capacity becomes positive around $N \sim 10^4$, and 2) the secure key capacity approaches its asymptotic value rather quickly.

The largest differences between the discrete variable QKD [4, 5] calculation and the DO-QKD calculation are the fluctuations in the error rates (discrete variable QKD) and the secret fraction (DO-QKD). According to [4], the dominant finite-key corrections are due to the fluctuations in the observed error rates. This is most likely the cause of the different behaviors for low N.

3 Experimental QKD Developments

3.1 Implementation of the Franson interferometer-based security check in the PIC

The interference of information-carrying quantum states is critical to many studies in applied and fundamental quantum communication. This interference can be used to test the correlations between distant states and bound the information gained on these states by an eavesdropper (E91, Howell 2007), and can be related to the channel capacity.

Because this quantum interference is performed between spatially-separated information carriers (i.e. photons), an interferometer relying on non-local interference is of great importance. A Franson interferometer is such a device, measuring the fourth-order temporal correlation function of biphoton entangled states.

Franson interferometry has been performed in free space and in fibers (Wong, 2012), however we chose to use silicon photonic integrated circuits (PIC). PICs offer superior phase stability and enable the scaling of quantum processing systems by leveraging the advanced silicon nanofabrication infrastructure. The PICs and supporting optical setup are shown in Fig. 2. We generated energy-time entangled photon pairs by type-II spontaneous parametric down conversion, spectrally filtered the photon pairs and then separated them with a polarizing beam splitter. One photon of each pair was sent to a PIC signifying both Alice and Bob, containing an unbalanced Mach-Zehnder interferometer (MZI) with a path imbalance of 200 ps.

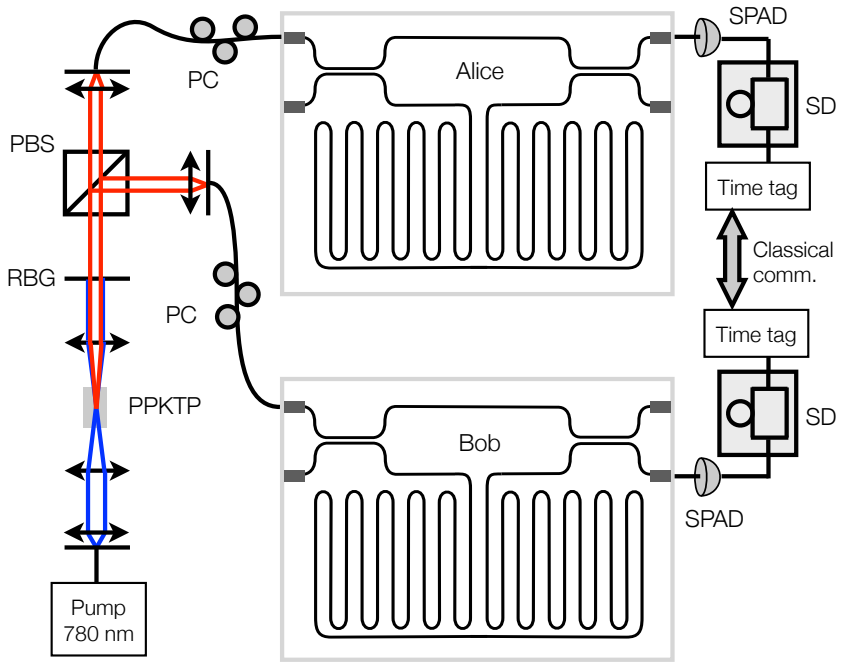

Figure 2: Franson interferometers consisting of two PIC-based Mach-Zehnder interferometers.

Due to loss in the waveguides amounting to 4 dB attenuation in the long arm of the MZIs, the splitting ratios of the directional couplers needed to be adjusted to maintain high visibility. We tested the classical visibility of a single unbalanced MZI using a long coherence-time laser, and achieved between 97% and 99% for a given splitting ratio. An example transmission plot is shown in Fig. 3(a) as a function of the interferometer temperature. Using these optimized structures, we then performed the Franson interference measurement and achieved the results shown in Fig. 3(b), using a custom feedback circuit to lock the temperature of the two silicon chips. We achieve close to 60% visibility.

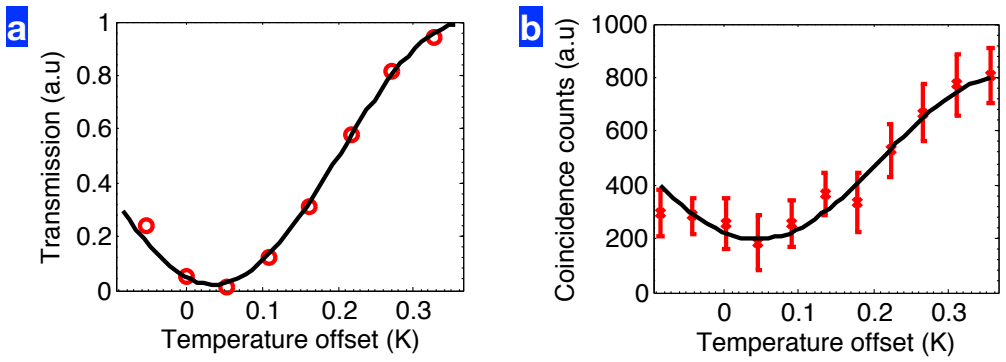

Figure 3: Coincidence measurements for PIC-based Franson interference experiment. (a) First-order coherence function of one of the two PIC circuits as temperature difference between Alice's and Bob's PICs is varied. (b) Second-order coherence function $g^{(2)}(\tau)$ as a function of the temperature offset between Alice's and Bob's PICs.

3.2 Waveguide-SNSPD Development

We fabricated and characterized SNSPDs on SiNx for the QuCIP program. These detectors will be released on membranes and integrated with waveguides. SEMs of waveguide-SNSPDs (WG-SNSPDs) are shown in Fig. 4. The size of the detector (marked in yellow in Fig. 4(a)) was constrained by the accuracy of membrane placement ($\pm$0.5μm), the width of the waveguide (~0.5μm) and the required waveguide-to-nanowire coupling length ($\geq$20μm for >90% optical absorption and nanowire widths larger than 60nm, according to simulations). The current device design ensures dual-pass waveguide-nanowire overlap, i.e. 30μm of waveguide-to-nanowire coupling length.

The detectors were characterized at 2.4 Kelvin. The critical currents (IC, defined as the maximum detector bias current IB) ranged from 7μA for 47-nm –wide nanowires to 14.9μA for 95-nm-wide nanowires. The back-illuminated device detection efficiency vs bias current is shown in Fig. 5(a). The measurements were performed using an incoherent polarized CW source with 1540nm center wavelength. The numbers agree well with absorption numbers (~3%-7%) obtained from optical simulations for back-illuminated devices on SiNx. Since we will not back-illuminate these detectors, but will couple the light evanescently, we can factor out the effect of back-illuminated absorption. The device property that is important for our experiments is the 'internal efficiency', also called 'propability of resistive state formation PR'. PR is the probability that the SNSPD produces an output signal once the detector

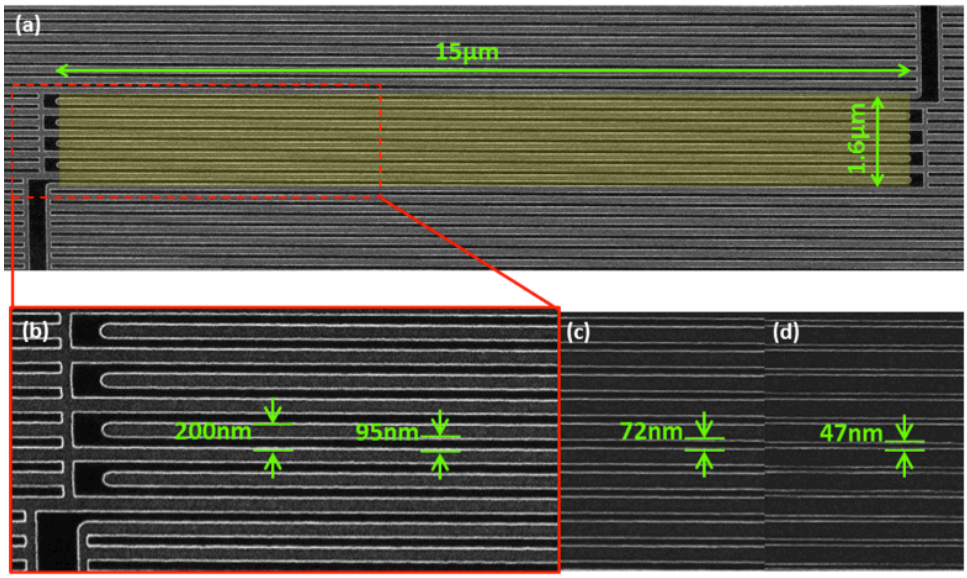

Figure 4: SEMs of WG-SNSPD HSQ masks on top of NbN. (a,b) WG-SNSPD based on 95-nm-wide nanowires. The active area of the detector is marked in yellow. The pitch was 200nm and the length of the meander structure was 15µm, resulting in a waveguide-to-nanowire coupling length of 30µm when the detector is placed on top of a 500-nm-wide waveguide. (c,d) Portion of WG-SNSPD based on 72- and 47-nm-wide nanowires.

has optically been absorbed in the nanowire. We can estimate PR by dividing the device detection efficiency by the calculated optical absorption. The results are shown in Fig. 5(b). Narrower nanowires reach the maximum internal efficiency (>90%) at lower bias currents and show a roughly constant ('saturated') detection efficiency close to the critical current. This behavior is preferable because it means that the device can reach near-unity internal efficiency even if the critical current is suppressed due to higher base temperature (which is >3K in one of the systems that we will use, as outlined in section 3). However, the disadvantage of narrow nanowires is the low signal amplitude (which is proportional to the bias current). As shown in Fig. 6, a lower signal-to-noise ratio results in higher timing jitter. For waveguide-integration, we will use detectors with critical currents beyond 13µA in order to ensure sub-35-ps timing jitter.

3.2.1 Membrane process

Fig. 7(a) shows a membrane-SNSPD fabricated using the old process. These detectors could not be tested after membrane undercut (prior to transfer) to confirm that they were not damaged during the membrane fabrication process. We solved this issue by modifying the membrane design. Fig. 7(b) shows a membrane-SNSPD (HSQ mask on NbN acting as dummy SNSPDs) fabricated using the new process. Two ~5-µm-wide leads connect the small gold pads on the membrane with larger gold pads on the surrounding bulk substrate, enabling testing of membrane-SNSPDs before transfer.

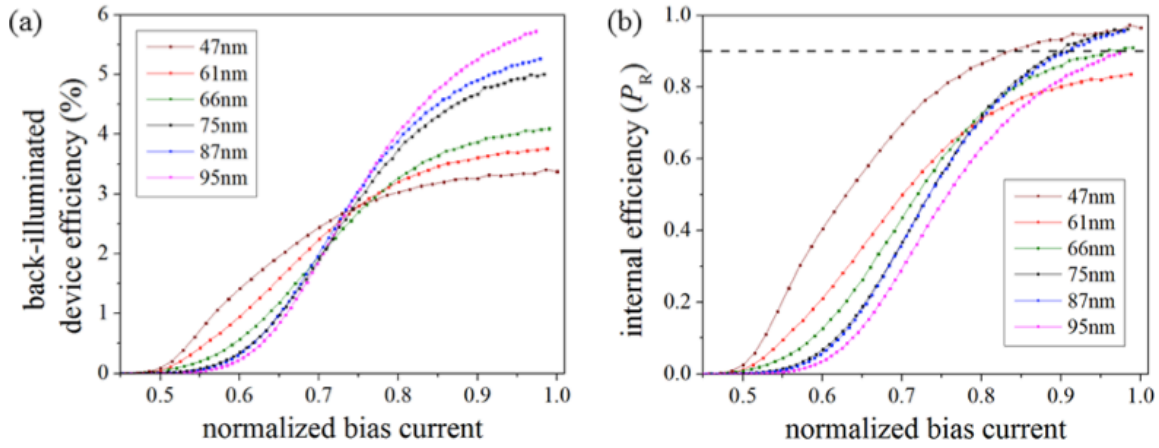

Figure 5: (a) Back-illuminated device detection efficiency vs bias current (IB) normalized by critical current (IC). The detection efficiency is plotted for nanowire widths 47nm (IC =7μA), 61nm (IC =7.9μA), 66nm (IC=10.1μA), 75nm (IC=12.2μA), 87nm (IC=13.8uA) and 95nm (IC=14.9μA). (b) The calculated internal efficiency (PR) of the same detectors as in (a).

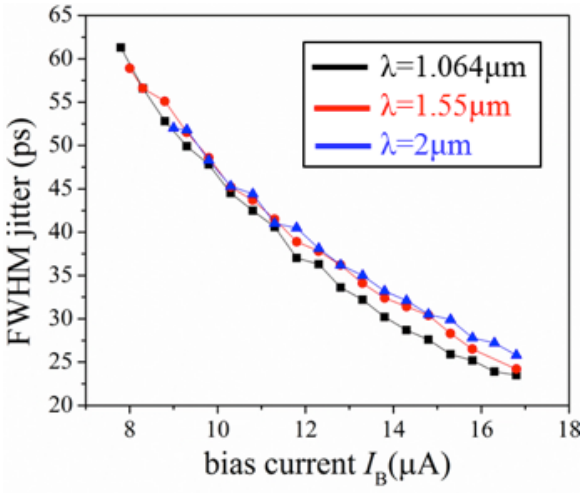

Figure 6: SNSPD timing jitter (FWHM) vs SNSPD bias current. The measurements were performed at 2.4K.

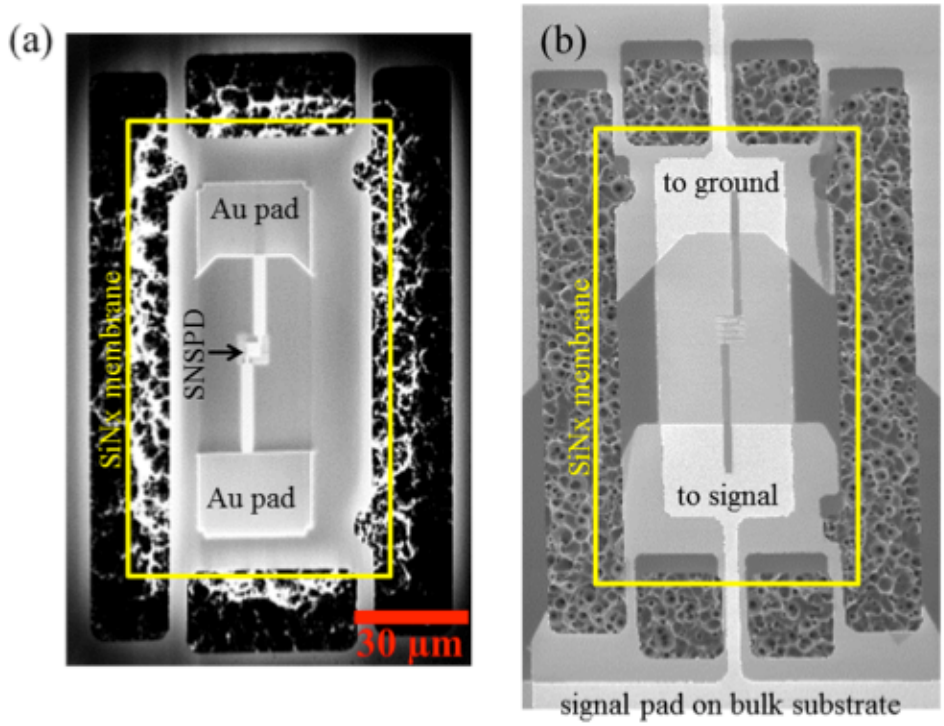

Figure 7: SEM of membrane-SNSPD showing the old (a) and the new design (b). In the new design two narrow leads connect the gold pads on the membrane to larger pads on the surrounding bulk substrate.

3. Efficient fiber-coupling to waveguide chip

We are pursuing a dual approach to efficient fiber-to-waveguide coupling. The goal is to achieve sub-3-dB fiber-to-waveguide coupling loss. One approach, shown in

Fig. 8 (a,b), is a mode-field-diameter (MFD)-shrinking coupler that is aligned and glued to the taper of the Silicon waveguide. The alignment is performed by ChiralPhotonics, Inc. We are planning to integrate this package with our dip probe, which will allow liquid-helium-emersion operation of waveguide-SNSPDs at 1.6 Kelvin. However, there is the possibility of misalignment between the coupler and the chip due to thermal expansion and continuous thermal cycling. We are currently investigating the robustness of this package during thermal cycling.

Due to the limited operation time in our immersed liquid helium system, we are also evaluating a second approach, shown in Fig. 8(c), which includes using 3-axis piezo stages in a closed-cycle cryostat to side-couple a lensed fiber to the waveguide chip. The disadvantage of this setup is the elevated base temperature of 3 Kelvin.

4 Publications and Presentation

Tian Zhong of MIT presented a poster on the dispersion compensation for the Franson interferometer at the 11th Conference on Quantum Communication, Measurement, and Computing in Vienna, Austria, August 2012.

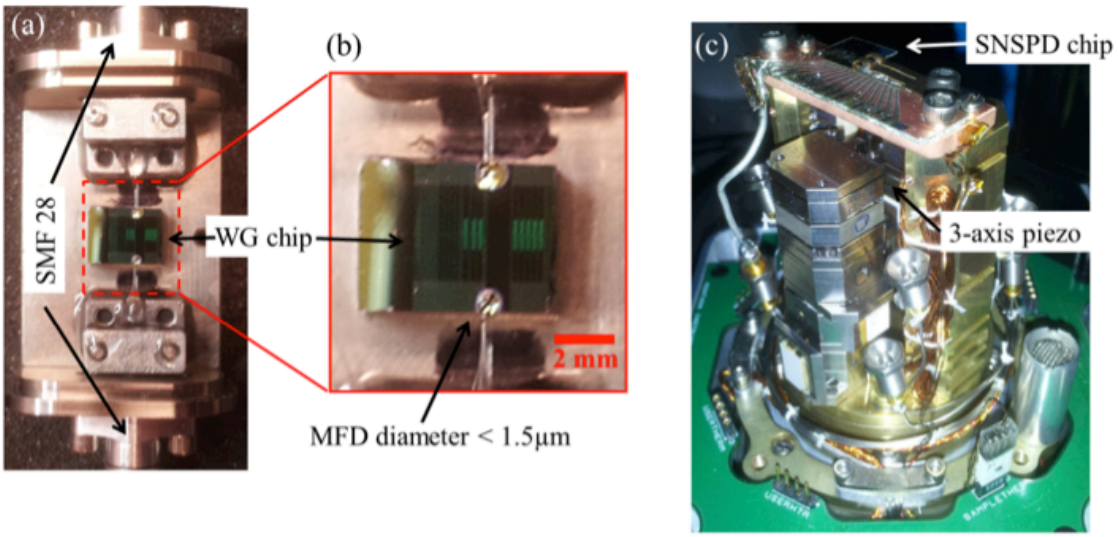

Figure 8: (a, b) Fiber-chip package. The coupler shrinks the MFD of the single-mode fiber to less than 1.5μm, enabling efficient coupling into the tapered waveguides on the Silicon chip in the center of the package. The coupler was aligned and glued to the waveguide by ChiralPhotonics, Inc. (c) Piezo stages on the cold head of a closed-cycle cryostat. The waveguide-SNSPD chip is mounted on a platform and the piezo stages are used to side-couple a lensed fiber to the waveguides.

4.1 Journal Publications

- Directional free-space coupling from photonic crystal waveguides, C.-C. Tsai, J. Mower, and D. Englund, Optics Express 19 (21), 20586-96 (2011)
- Efficient generation of single and entangled photons on a silicon photonic integrated chip, J. Mower and D. Englund, Phys. Rev. A 84, 052326 (2011)
- Wavelength Division Multiplexed Quantum Key Distribution, J. Mower, F. Wong, J. Shapiro, D. Englund, ArXiv:1110.4867 (2011)
- Zero phase delay in negative-index photonic crystal superlattices, S. Kocaman, M.S. Aras, P. Hsieh, J. F. McMillan, C. G. Biris, N. C. Panoiu, M. B. Yu, D. L. Kwong, A. Stein, and C. W. Wong, Nature Photonics 5, 499 (2011).
- "High-dimensional quantum key distribution using dispersive optics", J. Mower, P. Desjardins, J. H. Shapiro, D. Englund, under review at Phys. Rev. Lett. (2012)
- Private-Capacity Bounds for Bosonic Wiretap Channels, Ligong Wang, Jeffrey H. Shapiro, Nivedita Chandrasekaran, and Gregory W. Wornell, ArXiv:1202.1126 (2012)
- "Efficient single-spatial-mode periodically poled $KTiOPO_4$ waveguide source for high-dimensional entanglement-based quantum key distribution." Co-authors include Alessandro Restelli and Josh Biefang of NIST. Manuscript is under NIST review; we expect to submit it to Optics Express in early September.

- Chip-scale HOM visibility in infrared, accepted for publication in Optics Express 2013. [F. Wong, Englund, C. W. Wong groups].

- "Achieving multiple secure bits per coincidence in time-energy entanglement based quantum key distribution", Zheshen Zhang, Franco N. C. Wong, Jeffrey H. Shapiro, to be submitted (2013)

5 Conference Papers

- T. Zhong, F. N. C. Wong, A. Restelli, and J. C. Biefang, "Efficient single-spatial-mode PPKTP waveguide source for high dimensional entanglement-based QKD," to be presented at CLEO/QELS 2012, paper JTh1K3.

- eT. Zhong and F. N. C. Wong, "Franson interferometry with 99.6% visibility via fiberoptic dispersion engineering," in 11th International Conference on Quantum Communication, Measurement and Computing, Vienna, Austria, July 2012, paper accepted for presentation.

- D. Englund and J. Mower, "Quantum Optics on Silicon Photonic Chips", Invited Paper at Frontiers In Optics (San Jose, CA, Oct. 18, 2011)

- On High-Efficiency Optical Communication and Key Distribution, Yuval Kochman and Gregory W. Wornell, ITA, San Diego (2012)

- Private-Capacity Bounds for Bosonic Wiretap Channels, Ligong Wang, Jeffrey H. Shapiro, Nivedita Chandrasekaran, and Gregory W. Wornell, submitted to IEEE International Symposium on Information Theory (2012)

- F. N. C. Wong, "Time-energy entangled waveguide source for high-dimensional QKD," in Laser Science XXVII, San Jose, CA, October 2011, invited paper $LTuF_4$.

- J. Mower and D. Englund, "High-dimensional quantum key distribution using dispersive optics," submitted for Frontiers in Optics, Rochester, NY, 2012

- Mode-locked two-photon state, with HOM revival in 16 frequency bins – in preparation for Phys. Rev. series submission [Columbia + MIT groups]. 2013 CLEO submission prepared.

- Xiaolong Hu, Xiang Mao, Jacob Mower, Catherine Lee, Prashanta Kharel, Zhenda Xie, XinAn Xu, Chee Wei Wong, and Dirk Englund. Nonlocal cancellation of multi-frequency- channel dispersion yields double coincidence peaks. submitted to CLEO, 2013.

References

[1] Jacob Mower, Pierre Desjardins, Zheshen Zhang, Catherine Lee, Jeffrey Shapiro, and Dirk Englund. Large-alphabet quantum key distribution using dispersive optics. *under review*, 2012.

[2] Zheshen Zhang, Franco N. C. Wong, and Jeffrey H. Shapiro. Achieving multiple secure bits per coincidence in time-energy entanglement based quantum key distribution. *to be submitted*, 2013.

[3] Xiaolong Hu, Xiang Mao, Jacob Mower, Catherine Lee, Prashanta Kharel, Zhenda Xie, XinAn Xu, Chee Wei Wong, and Dirk Englund. Nonlocal cancellation of multi-frequency-channel dispersion yields double coincidence peaks. *submitted to CLEO*, 2013.

[4] Lana Sheridan and Valerio Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82:030301, Sep 2010.

[5] Lana Sheridan and Valerio Scarani. Erratum: Security proof for quantum key distribution using qudit systems [Phys. Rev. A 82, 030301(R) (2010)]. *Phys. Rev. A*, 83:039901, Mar 2011.

[6] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.